UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/817,288	03/27/2001	Yoshitake Shinkai	826.1718	7742

21171 7590 12/20/2005

STAAS & HALSEY LLP
SUITE 700
1201 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
LESNIEWSKI, VICTOR D	

ART UNIT	PAPER NUMBER
2152	

DATE MAILED: 12/20/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/817,288	SHINKAI ET AL.	
	Examiner	Art Unit	
	Victor Lesniewski	2152	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 October 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8,10-12,14 and 16-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8,10-12,14 and 16-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The amendment filed 9/6/2005 has been placed of record in the file.

2. Claims 1-8, 10-12, 14, 16, 17, and 20-28 have been amended.

3. Claims 9, 13, 15, and 29 have been canceled.

4. Claims 1-8, 10-12, 14, and 16-28 are now pending.

5. The applicant's arguments with respect to claims 1-8, 10-12, 14, and 16-28 have been considered but are moot in view of the following new grounds of rejection.

Continued Examination Under 37 CFR 1.114

6. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous office action has been withdrawn pursuant to 37 CFR 1.114. The applicant's submission filed on 10/19/2005 has been entered.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1-3, 8, 10-12, 14, 23, 25, 27, and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Slaughter et al. (U.S. Patent Number 5,964,886) in view of Loucks et al. (U.S. Patent Number 5,634,122), hereinafter referred to as Loucks.

9. Slaughter disclosed a virtual disk system that provides consistent data to a plurality of nodes in a cluster. In an analogous art, Loucks disclosed a distributed file system that uses a local token manager to resolve token conflicts before granting tokens.

10. Concerning the independent claims, Slaughter did not explicitly state a token manager that gives access permission for a file when no other node has update permission. Although Slaughter's system does set forth different types of access permissions, the system is mainly focused on accessing storage devices found to be available or in an active state. However, Loucks remedies the token manager issue as his system (also focused on accessing a file on a storage device) utilizes a manager to grant or deny tokens to requesting network nodes. Similarly, since Slaughter does not deal explicitly with tokens, Slaughter also does not state notifying the requesting node of another node that has a token. However, Slaughter does operate similarly in that his system maintains a list of active devices and when needed informs the requesting node of an alternate node through which the requested file can be accessed. Thus, it would be a simple extension of Slaughter's system to use a token manager, such as the one presented by Loucks, in conjunction with or instead of the active device list and then base the system on a required token. Said another way, Slaughter's system accesses file storage devices based on availability. Slaughter explicitly discusses availability in terms of an active network connection or the failure of a network connection. However, another type of availability is whether or not the device is available based on which node has a required token. Here, Loucks'

token system can be utilized with Slaughter to determine a certain availability while Slaughter's system would still maintain its operating logic in accessing the storage devices. For more detail, see the specific line citations below. Thus, it would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to modify the system of Slaughter by adding the ability to utilize a token manager as claimed (for such purposes as giving access permission for a file when no other node has update permission and notifying the requesting node of another node that has a token) as provided by Loucks. Here the combination satisfies the need for a virtual disk system that ensures that each node has consistent permission data. See Slaughter, column 2, lines 25-29. This rationale also applies to those dependent claims utilizing the same combination.

11. Thereby, the combination of Slaughter and Loucks discloses:

- <Claims 1 and 10>

  (presented together since they disclose similar limitations)

  A file replication system having a plurality of nodes connected to a network, files being distributed to the nodes, wherein a first node of the nodes comprises: a first token managing portion giving access permission for a file within the first node when no other node has update permission and otherwise issuing a notification of a permitted node that has update permission for the file in response to an access request in first node (Slaughter, column 9, lines 24-27 and 36-47 and Loucks, figure 8b), and an IO request intercepting portion accepting an access to the file, the access taking place in the first node when said IO request intercepting portion is capable of acquiring the access permission, asking said first token managing portion to acquire the access permission

against the access request, and asking the permitted node that has update permission for the file to access to the file when said first token managing portion is not capable of acquiring the access permission (Slaughter, column 9, lines 27-35; column 10, lines 16-28; and column 8, lines 13-26), and a second node comprises a second token managing portion notifying a requesting node that requests the access permission for the file of the permitted node that has the update permission for the file as a response message (Slaughter, column 8, lines 33-41 and Loucks, column 6, lines 36-49).

- <Claims 2 and 11>

  A node, connected to at least one other node through a network, every node having a copy of files synchronized with files of other nodes for high availability and high performance to provide a replicated file system, comprising: a token managing portion managing an access request for a file (Loucks, column 6, lines 36-49); and an IO request intercepting portion asking said token managing portion to acquire an access permission for the file against an access request to the file in said node, said token managing portion giving access permission when no other node has update permission for the file and said token managing portion notifying said IO request intercepting portion of another node that has the update permission when the other node has the update permission for the file, in response to the access request of said IO request intercepting portion, said IO request interception portion accessing the file in said node when the IO request intercepting portion is capable of acquiring the access permission and said IO request intercepting portion asking the other node that has the update permission to access the file instead of accessing the file in said node when said IO request intercepting portion is not capable of

acquiring the access permission (Slaughter, column 9, lines 24-47; column 10, lines 16-28; and column 8, lines 13-26 and Loucks, figure 8b).

- <Claim 3>

  The node according to claim 2, further comprising: a system structure managing portion performing a restoration process of data of a file of the node when it is newly joined to a system (Slaughter, column 8, lines 42-49), wherein while said system structure managing portion is restoring the file, when an access request for the file takes place in the node, said IO request intercepting portion asks another node that shares the file to access the file (Slaughter, column 10, lines 30-43).

- <Claims 8 and 12>

  A node, connected to at least one other node through a network, every node having a copy of files synchronized with files of other nodes for high availability and high performance to provide a replicated file system, comprising: a token managing portion asking another node to acquire an access permission for a file against an access request for the file in said node (Slaughter, column 9, lines 27-35 and column 10, lines 16-28); and an IO request intercepting portion accepting an access request for a file in said node, asking said token managing portion to acquire the access permission for the file against the access request to the file in said node, said token managing portion giving access permission when no other node has update permission for the file and otherwise notifying said IO request intercepting portion of another node that has the update permission for the file, said IO request intercepting portion accessing the file in said node when the IO request intercepting portion is capable of acquiring the access permission and asking the

other node that has the update permission for the file to access the file according to the access request instead of accessing the file in said node when said token managing portion is not capable of acquiring the access permission for the file (Slaughter, column 9, lines 24-47; column 10, lines 16-28; and column 8, lines 13-26 and Loucks, column 6, lines 23-49 and figure 8b).

- <Claim 14>

  A file replication control method for a system having a plurality of nodes connected to a network, files being distributed to the nodes, comprising: causing an access requesting node to access a file of the access requesting node itself when the access requesting node has the latest data of the file and has or is able to obtain access permission from another node having update permission for the file; and asking the other node to access the file when the other node has the update permission for the file which is given to only one node at a time (Slaughter, column 9, lines 24-47 and column 10, lines 16-28 and Loucks, column 6, lines 36-49 and figure 8b).

- <Claim 23>

  The file replication control method according to claim 14, further comprising: restoring data of a file of a newly joined node (Slaughter, column 8, lines 42-49); and operating a user program before data of the file is completely restored (Slaughter, column 10, lines 30-43).

- <Claim 25>

  The file replication control method according to claim 23, wherein the node asks another node that shares the file to perform a process for an access request for the file when the

access request takes place in the node itself before data is completely restored (Slaughter, column 10, lines 30-43).

- <Claim 27>

  A file replication method for a system having a plurality of nodes connected to a network, files being distributed to the nodes, comprising: causing a first node to request a token for accessing a file (Loucks, column 6, lines 36-49); causing the first node to access the file when the first node has the latest data of the file and is able to obtain the token for accessing the file from another node having update permission for the file which is given to only one node at a time (Slaughter, column 9, lines 24-27 and 36-47 and Loucks, figure 8b); notifying the first node of a second node that has the token when the first node is not capable of acquiring the token (Slaugher, column 8, lines 33-41 and Loucks, column 6, lines 36-49); and causing the first node to ask the second node to access the file when the first node is notified that the first node is not capable of acquiring the token (Slaughter, column 9, lines 27-35 and column 10, lines 16-28).

- <Claim 28>

  A computer-readable portable storage medium, when being used by a computer that composes a node connected to other nodes through a network in a file replication system, on which is recorded a program for causing the computer to execute a process, said process comprising: when the node accesses a file and a node itself has the latest data of the file and has or is able to obtain access permission from another node having update permission for the file, causing the node itself to access the shared file of the node itself (Slaughter, column 9, lines 24-27 and 36-47 and Loucks, figure 8b); and when another

node has the update permission for the file which is given to only one node at a time, causing the node itself to ask the other node to access the file (Slaughter, column 9, lines 27-35 and column 10, lines 16-28 and Loucks, column 6, lines 36-49).

Since the combination of Slaugher and Loucks discloses all of the above limitations, claims 1-3, 8, 10-12, 14, 23, 25, 27, and 28 are rejected.

12. Claims 4-7, 16-22, 24, and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Slaughter in view of Loucks, as applied above, further in view of Tavares et al. (U.S. Patent Number 5,515,537), hereinafter referred to as Tavares.

13. The combination of Slaughter and Loucks disclosed a virtual disk system that provides consistent data to a plurality of nodes in a cluster and uses a token manager to resolve token conflicts before granting tokens. In an analogous art, Tavares disclosed a method of sharing data between processors on the same network by using a real-time distributed locking system. Both systems focus on data sharing and methods to allow users access to certain data.

14. Concerning claims 4, 16, 17, and other related dependents such as claims 21, 22, and 24, although the combination of Slaughter and Loucks states updating content in each node of the virtual disk system, it did not explicitly state propagating updated content of the file to other nodes as claimed or the update's dependent relationship between nodes as claimed. However, Tavares does state a system wherein update data is propagated throughout the system as claimed. See figure 7. Furthermore, Tavares sends updated content and also passes a token from one node to the next in an ordered fashion based on the physical architecture of the system or on the processing of queues. It would have been obvious to one of ordinary skill in the art at the time of

the applicant's invention to modify the combination of Slaughter and Loucks by adding the ability to propagate updated content of the shared file to other nodes and utilize an update's dependent relationship between nodes as provided by Tavares. Here the combination satisfies the need for a file replication system that ensures that each node has consistent permission data. See Slaughter, column 2, lines 25-29. This rationale also applies to those dependent claims utilizing the same combination.

15. Thereby, the combination of Slaughter, Loucks, and Tavares discloses:

- <Claim 4>

  The node according to claim 2, further comprising: a changed data notifying portion propagating an updated content of the file to other node along with information that represents a dependent relationship with another update (Tavares, column 6, lines 55-59); and a received data processing portion reflecting the updated content to the shared file while assuring an order of the update based on the dependency relationship (Tavares, column 8, lines 12-15).

- <Claim 5>

  The node according to claim 4, further comprising: a system state information portion storing information about propagation mode of an updated content for each of at least one file, wherein said changed data notifying portion propagates the update content based on information queued in said system information portion (Tavares, column 9, line 60 through column 10, line 20).

- <Claim 6>

  The node according to claim 5, wherein the propagation mode is one of a synchronous mode in which it is assured that the updated content is propagated to all the nodes that share the file, a semi-synchronous mode in which it is assured that the updated content is propagated to the majority of nodes that share the file, and an asynchronous mode in which it is not acknowledged that the updated content is propagated to the nodes that share the file (Tavares, column 9, lines 60-66).

- <Claim 7>

  The node according to claim 4, wherein said system state information storing portion keeps information about each node that shares at least one file for each file (Tavares, column 10, lines 6-9).

- <Claim 16>

  The file replication control method according to claim 14, wherein the other node that has the update permission releases the update permission after an update that has a dependent relationship with the update performed at the other node has been propagated to all the nodes (Tavares, column 7, lines 37-39).

- <Claim 17>

  The file replication control method according to claim 14, wherein said method further comprises: the other node that has updated the file asynchronously propagating an updated content to the other nodes; and causing the other node that has updated the file to process an access request that takes place in the access requesting node while the updated content is being propagated (Tavares, column 10, lines 15-20).

- <Claim 18>

  The file replication control method according to claim 17, wherein the updated content is reflected in such a manner that order thereof is assured (Tavares, column 7, lines 2-16).

- <Claim 19>

  The file replication control method according to claim 18, wherein a dependency information that represents order of other updates to be propagated to the other node along with the updated content (Tavares, column 8, lines 12-15).

- <Claim 20>

  The file replication control method according to claim 19, wherein a node that has received the updated content to reflect the updated content on a file of the node itself after receiving a previous updated content based on the dependency information (Tavares, column 10, lines 15-20).

- <Claim 21>

  The file replication control method according to claim 14, wherein a propagation mode of an updated content is designated for each of at least one file (Tavares, column 9, lines 60-66).

- <Claim 22>

  The file replication control method according to claim 14, wherein a node to which an updated content is propagated is designated for each of at least one file (Tavares, column 7, lines 2-16).

- <Claim 24>

  The file replication control method according to claim 23, wherein restored data is transmitted in such a manner that order of update requests for the file is assured (Tavares, column 8, lines 12-15).

- <Claim 26>

  The file replication control method according to claim 14, wherein a node that has performed a systematic stop in which nodes that share a file are synchronously stopped to store a systematic stop state and the node synchronously resumes a process for the file without restoring data of the file (Tavares, column 9, lines 60-66).

Since the combination of Slaughter, Loucks, and Tavares discloses all of the above limitations, claims 4-7, 16-22, 24, and 26 are rejected.

Conclusion

16. The prior art made of record and not relied upon is considered pertinent to the applicant's disclosure.

- Johnson et al. (U.S. Patent Number 5,175,852) disclosed a distributed file management system that uses administrative information to manage local files and files existing on other nodes.
- Foulston (U.S. Patent Number 5,884,308) disclosed a method for updating distributed data files using an active token distribution scheme.

- DeKoning et al. (U.S. Patent Number 5,933,824) disclosed a method for coordinating file lock requests from a cluster of attached host computers within I/O controllers attached to a storage system.
- Burnett et al. (U.S. Patent Number 6,006,018) disclosed a method for providing authenticated access to files stored in a target distributed file system in response to file requests originating from clients associated with a source distributed file system.
- Berbec et al. (U.S. Patent Number 6,122,631) disclosed a method for dynamically controlling access to files in a client/server system that uses an object server which generates tokens for the files.
- Oak (U.S. Patent Number 6,954,895) disclosed a method for storing objects wherein object data is stored separately from a file containing an instance of the object and access permissions are required for access to the stored object.

17. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Victor Lesniewski whose telephone number is 571-272-3987. The examiner can normally be reached on Monday through Thursday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Bunjob Jaroenchonwanit can be reached on 571-272-3913. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Victor Lesniewski
Patent Examiner
Group Art Unit 2152

BUNJOB JAROENCHONWANIT
PRIMARY EXAMINER